

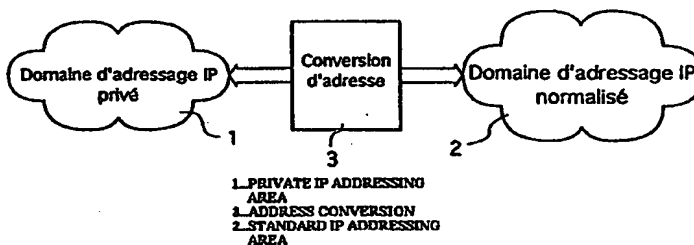


DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : H04L 29/06, 12/66	A1	(11) Numéro de publication internationale: WO 97/05727 (43) Date de publication internationale: 13 février 1997 (13.02.97)
(21) Numéro de la demande internationale: PCT/FR96/01179 (22) Date de dépôt international: 25 juillet 1996 (25.07.96) (30) Données relatives à la priorité: 95/09392 27 juillet 1995 (27.07.95) FR (71)(72) Déposant et inventeur: ALEXANDRE, Serge [FR/FR]; 26, Villa Raspail, F-92160 Antony (FR). (74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Im- meuble Germanium, 80, avenue des Buttes-de-Coësmes, F- 35700 Rennes (FR).	(81) Etats désignés: AL, AM, AT, AT (modèle d'utilité), AU, AZ, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (modèle d'utilité), DE, DE (modèle d'utilité), DK, DK (modèle d'utilité), EE, EE (modèle d'utilité), ES, FI, FI (modèle d'utilité), GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (modèle d'utilité), TJ, TM, TR, TT, UA, UG, US, UZ, VN, brevet ARIPO (KE, LS, MW, SD, SZ, UG), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Publiée Avec rapport de recherche internationale.	

(54) Title: NETWORK INTERCONNECTION ROUTER, METHOD AND DEVICE

(54) Titre: DISPOSITIF, PROCÉDE ET ROUTEUR D'INTERCONNEXION DE RESEAUX



(57) Abstract

A method for interconnecting networks which use internet technology, whereby a first network (1) with private IP addressing may be linked with a second network (2) with standard IP addressing. Said first and second networks convey packets that each comprise an IP header including, in particular, a "source IP address" field and a "destination IP address" field. The packets are considered as outbound when they are moved from the first network (1) to the second network (2) via the device, and inbound when the reverse is the case. For each outbound packet, the method comprises a first step of converting the private IP address in the "source IP address" field so that after conversion, said "source IP address" field contains a single intermediate standard IP address. For each inbound packet, the method further comprises a second step of converting the single intermediate standard IP address in the "destination IP address" field so that after conversion, said "destination IP address" field of said inbound packet contains one of the private addresses of the first network.

(57) Abrégé

L'invention concerne un procédé d'interconnexion de réseaux mettant chacun en œuvre la technologie internet, du type permettant d'interconnecter un premier réseau (1) présentant un adressage IP privé et un second réseau (2) présentant un adressage IP normalisé, lesdits premier et second réseaux véhiculant des paquets, chacun desdits paquets comportant un en-tête IP comprenant notamment un champ "adresse IP source" et un champ "adresse IP destination", les paquets étant dits sortants s'ils se déplacent du premier (1) vers le second (2) réseau à travers ledit dispositif et sortants dans le cas contraire. Le procédé de l'invention comprend, pour chaque paquet sortant, une première étape de conversion de l'adresse IP privée contenue dans ledit champ "adresse IP source", de façon que ledit champ "adresse IP source" dudit paquet sortant contienne, après conversion, une adresse IP normalisée intermédiaire et unique. Le procédé de l'invention comprend également, pour chaque paquet entrant, une seconde étape de conversion de l'adresse IP normalisée intermédiaire et unique contenue dans le champ "adresse IP destination", de façon que ledit champ "adresse IP destination" dudit paquet entrant contienne, après conversion, une des adresses privées du premier réseau.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Arménie	GB	Royaume-Uni	MW	Malawi
AT	Autriche	GE	Géorgie	MX	Mexique
AU	Australie	GN	Guinée	NE	Niger
BB	Barbade	GR	Grèce	NL	Pays-Bas
BE	Belgique	HU	Hongrie	NO	Norvège
BF	Burkina Faso	IE	Irlande	NZ	Nouvelle-Zélande
BG	Bulgarie	IT	Italie	PL	Pologne
BJ	Bénin	JP	Japon	PT	Portugal
BR	Brésil	KE	Kenya	RO	Roumanie
BY	Bélarus	KG	Kirghizistan	RU	Fédération de Russie
CA	Canada	KP	République populaire démocratique de Corée	SD	Soudan
CF	République centrafricaine	KR	République de Corée	SE	Suède
CG	Congo	KZ	Kazakhstan	SG	Singapour
CH	Suisse	LI	Liechtenstein	SI	Slovénie
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovaquie
CM	Cameroun	LR	Libéria	SN	Sénégal
CN	Chine	LT	Lituanie	SZ	Swaziland
CS	Tchécoslovaquie	LU	Luxembourg	TD	Tchad
CZ	République tchèque	LV	Lettonie	TG	Togo
DE	Allemagne	MC	Monaco	TJ	Tadjikistan
DK	Danemark	MD	République de Moldova	TT	Trinité-et-Tobago
EE	Estonie	MG	Madagascar	UA	Ukraine
ES	Espagne	ML	Mali	UG	Ouganda
FI	Finlande	MN	Mongolie	US	Etats-Unis d'Amérique
FR	France	MR	Mauritanie	UZ	Ouzbékistan
GA	Gabon			VN	Viet Nam

DISPOSITIF, PROCEDE ET ROUTEUR D'INTERCONNEXION DE RESEAUX

Le domaine de l'invention est celui des réseaux de télécommunication mettant en oeuvre la technologie internet.

5 Plus précisément, l'invention concerne un dispositif et un procédé d'interconnexion de deux réseaux mettant chacun en oeuvre la technologie internet, l'un présentant un adressage IP privé et l'autre un adressage IP normalisé.

La technologie internet, aussi appelée technologie TCP/IP, est basée sur l'utilisation des protocoles TCP/IP qui se définissent comme une suite de protocoles
10 visant non seulement à interconnecter des calculateurs reliés par un même réseau physique, mais aussi à interconnecter ces différents réseaux physiques entre eux de manière à constituer un réseau logique unique.

Une des particularités marquantes de cette suite de protocoles est d'être indépendante du support physique, c'est-à-dire de fonctionner sur (et donc
15 d'interconnecter) toutes les technologies de support présentes et à venir (Ethernet, Token Ring, X.25, simple câble série, ATM, RNIS, Relais de Trames, etc...).

La technologie TCP/IP peut donc être employée par toute vaste organisation désirant uniformiser ses ressources réseaux, classiquement composées de plusieurs réseaux physiques, de technologies généralement différentes. Elle va ainsi permettre aux
20 utilisateurs et applications informatiques de faire apparaître ces éléments à priori incompatibles comme un réseau unique.

Il convient de distinguer la "technologie internet" du réseau Internet. Ce dernier est en fait un réseau mondial unique, interconnectant de très nombreuses machines et actuellement en très forte expansion.

25 Une organisation peut donc déployer son propre réseau sur la base de la technologie internet sans être connectée à Internet (le réseau mondial). Si elle souhaite ensuite s'y connecter, la tâche lui sera facilitée puisqu'elle utilise la même technologie.

Parmi la série de protocoles de transmission de données à laquelle fait référence TPC/IP, les plus importants sont :

30 - IP (pour Internet Protocol en anglo-saxon) ;

- TCP (pour Transmission Control Protocol en anglo-saxon) ;
- UDP (pour User Datagram Protocol en anglo-saxon).

Le protocole IP est le protocole de base de la technologie internet. Il a pour simple fonction de transférer un paquet de données (c'est-à-dire un ensemble d'octets) d'une machine à l'autre. Pour ce faire, il rajoute au paquet de données un en-tête IP comprenant notamment les trois champs suivants : "protocole", "adresse IP source" et "adresse IP destination".

En pratique, les données que véhicule un paquet IP sont en fait des unités de protocole d'un niveau supérieur (principe d'encapsulation), tels que TCP et UDP. Le champ "protocole" permet donc de définir ce protocole.

Les champs "adresse IP source" et "adresse IP destination" définissent l'adresse IP de la machine émettrice et de la machine destinatrice respectivement. Les adresses sont codées sur 32 bits. Dans le monde TCP/IP, une adresse définit à la fois la machine et le réseau physique auquel elle est raccordée. Elle est donc unique dans l'ensemble du réseau.

Lors de l'émission d'un paquet, une machine détecte (en comparant la partie des adresses définissant le réseau) si la machine destinatrice est sur le même réseau physique qu'elle même. Auquel cas, elle envoie directement le paquet. Sinon, elle l'envoie à une machine capable de faire suivre la paquet vers d'autres réseaux physiques. Une telle machine est généralement désignée par le terme de "routeur IP".

D'une façon générale, les communications entre équipements informatiques peuvent se classer en deux grandes familles, à savoir les communications en mode non-connecté et les communications en mode connecté.

Dans le mode non-connecté (appelé mode "connectionless", ou mode "datagram" par les anglo-saxons), la machine A désirant envoyer des données à la machine B constitue un élément de protocole incluant des données à transmettre, ainsi que l'adresse de la machine B. Le réseau se charge d'acheminer cet élément de protocole jusqu'à la machine destinatrice. Dans le monde TCP/IP, le protocole de transfert en mode non-connecté est UDP.

Le mode connecté est plus complexe que le précédent. Il introduit la notion de

connexion, analogue à une communication téléphonique. Une connexion a lieu entre deux équipements informatiques et comporte trois phases :

- l'établissement : la machine A demande l'établissement d'une connexion vers la machine B et celle-ci l'accepte ;
- 5 - le transfert : les machines A et B échangent des données au travers de cette connexion ;
- la libération : la connexion se termine sur l'initiative d'une des deux machines.

10 Une connexion est un objet abstrait concernant au moins les deux équipements d'extrémité. Ces équipements vont donc devoir créer, manipuler et effacer des structures de données décrivant l'état de la connexion.

Dans le monde TCP/IP, le protocole de transfert en mode connecté est TCP.

15 Lorsque l'on désire interconnecter plusieurs réseaux, il convient de s'assurer que le plan d'adressage de chacun des réseaux est compatible avec celui de chacun des autres réseaux.

Ainsi, dans le cas du réseau mondial Internet, constitué de plusieurs réseaux interconnectés, l'adressage IP est normalisé, de façon que chaque machine, quel que soit le réseau auquel elle appartient, possède une adresse IP distincte. Les instances administratives du réseau Internet sont seules habilitées à attribuer de nouvelle adresse IP.

20 Quand une organisation déploie son propre réseau (dit réseau privé) sur la base de la technologie internet, sans que ce réseau soit intégré au réseau mondial Internet, elle définit un plan d'adressage privé, qui est incompatible avec le plan d'adressage normalisé du réseau Internet. Si, ultérieurement, cette organisation décide de relier son réseau à adressage IP privé au réseau Internet, ou plus généralement à un réseau quelconque à adressage IP normalisé, elle se heurte à un problème d'incompatibilité entre les plans
25 d'adressage privé et normalisé.

Une première solution comme visant à pallier ce problème consiste à reconfigurer l'ensemble du réseau privé préalablement existant.

30 Cette première solution est très difficile à mettre en oeuvre puisque les instances administratives d'un réseau à adressage normalisé attribuent des espaces d'adressage ne

comprenant généralement qu'un faible nombre d'entrées. Ainsi, sur le réseau Internet, il est actuellement quasiment impossible d'obtenir des espaces d'adressage supérieurs à 256 entrées. En d'autres termes, il est impossible d'offrir des accès au réseau Internet à des réseaux privés existants comportant plus de 256 machines.

5 Par ailleurs, la logique de l'adressage IP étant symétrique, toute machine du réseau privé se mettant en situation d'accéder au réseau à adressage normalisé devient immédiatement accessible de l'extérieur à travers ce réseau à adressage normalisé. Or, une contrainte de l'administrateur du domaine d'adressage IP privé est généralement de maintenir la sécurité de son réseau. Il souhaite permettre aux machines de son réseau
10 privé d'accéder aux ressources disponibles sur le réseau normalisé. En revanche, il ne souhaite pas que les machines de ce réseau normalisé, donc extérieures, puissent accéder à l'ensemble des ressources de son réseau privé.

 Une seconde solution connue visant à pallier l'incompatibilité d'adressage entre deux réseaux à interconnecter consiste à interposer entre les deux réseaux un dispositif
15 réalisant une conversion d'adresses. Pour ce faire, le réseau privé doit donc se voir attribuer, par l'administrateur du domaine d'adressage IP normalisé, une adresse IP normalisée de raccordement, qui devra être affectée au dispositif de conversion d'adresse, et une plage d'adresses IP normalisées destinées à être affectées aux machines composant le réseau à raccorder.

20 Dans ce cas, une adresse IP normalisée est substituée de manière univoque à une adresse IP privée lors du passage des paquets au travers de la passerelle que constitue le dispositif d'interconnexion entre les deux réseaux.

 Cette seconde solution connue offre l'avantage, par rapport à la première, de ne pas nécessiter une renumérotation complète du réseau privé. En revanche, elle présente le
25 même inconvénient de nécessiter une plage d'adresses IP normalisées (au moins autant d'adresses normalisées que de machines composant le réseau privé) en plus de l'adresse de raccordement, ainsi que celui de ne pas assurer la sécurité du réseau privé (du fait de la symétrie de la logique d'adressage IP).

 Les passerelles applicatives constituent une troisième solution connue visant à
30 pallier l'incompatibilité d'adressage entre deux réseaux à interconnecter.

Cette troisième solution connue, si elle est performante sur le plan de la facilité d'administration et de la sécurité, présente les inconvénients suivants :

- un programme de relais applicatif est nécessaire pour chaque type d'application. La liste des services supportés est donc forcément réduite.
5 Et surtout, une passerelle applicative ne pourra pas, sauf mise à jour logicielle, supporter les nouveaux services Internet encore inconnus ou expérimentaux à ce jour ;
- le programme n'est pas transparent pour l'utilisateur. Il doit en effet se connecter sur la passerelle, et ensuite établir la connexion vers le service
10 désiré. Ceci pouvant être plus ou moins masqué par des protocoles spécifiques entre la passerelle et l'utilisateur. Mais, ensuite il est alors généralement nécessaire de modifier l'outil d'accès, ce qui interdit l'emploi de produits standards du marché.

15 L'invention a notamment pour objectif de pallier ces différents inconvénients de l'état de la technique.

Plus précisément, l'un des objectifs de la présente invention est de fournir un procédé de conversion d'adresse entre un premier réseau présentant un adressage IP privé et un second réseau présentant un adressage IP normalisé, ce procédé ne nécessitant pas l'attribution au réseau privé d'une plage d'adresses IP normalisées.

20 L'invention a également pour objectif de fournir un tel procédé qui permette d'interdire les connexions du réseau à adressage normalisé vers le réseau à adressage privé, de façon à assurer la sécurité du réseau privé.

Un autre objectif de l'invention est de fournir un tel procédé qui soit indépendant du type d'application et transparent pour les utilisateurs des machines du réseau privé.

25 Un objectif complémentaire de l'invention est de fournir un dispositif d'interconnexion d'adresses répondant aux objectifs précités.

Ces différents objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un procédé d'interconnexion de réseaux mettant
30 chacun en oeuvre la technologie internet, du type permettant d'interconnecter un premier réseau présentant un adressage IP privé et un second réseau présentant un adressage IP

normalisé, lesdits premier et second réseaux véhiculant des paquets, chacun desdits paquets comportant un en-tête IP comprenant notamment un champ "adresse IP source" et un champ "adresse IP destination", les paquets étant dits sortants s'ils se déplacent du premier vers le second réseau à travers ledit dispositif et entrants dans le cas contraire,

5 ledit procédé comprenant, pour chaque paquet sortant, une première étape de conversion de l'adresse IP privée contenue dans ledit champ "adresse IP source", de façon que ledit champ "adresse IP source" dudit paquet sortant contienne, après conversion, une adresse IP normalisée intermédiaire et unique ;

10 et ledit procédé comprenant, pour chaque paquet entrant, une seconde étape de conversion de l'adresse IP normalisée intermédiaire et unique contenue dans le champ "adresse IP destination", de façon que ledit champ "adresse IP destination" dudit paquet entrant contienne, après conversion, une des adresses privées du premier réseau.

15 Ainsi, le principe général de l'invention consiste à n'utiliser qu'une seule adresse IP normalisée. Vu du réseau normalisé, toutes les connexions provenant du réseau privé apparaissent comme provenant de cette adresse unique. Ceci permet une grande simplification de l'administration du dispositif qui met en oeuvre le procédé de l'invention, comme de l'administration de l'ensemble du réseau privé. De plus, le procédé de l'invention offre la possibilité de connexion à partir d'un simple accès de type "dialup-ip".

20 Dans un mode de réalisation préférentiel de l'invention, chacun desdits paquets comportant un en-tête TCP ou UDP comprenant notamment un champ "port source" et un champ "port destination", ledit en-tête IP comprenant en outre un champ "protocole de transport" indiquant le protocole TCP ou UDP utilisé, les paquets empruntant des connexions bidirectionnelles, chaque connexion étant un lien logique entre une première
25 extrémité du premier réseau et une seconde extrémité du second réseau, chaque première ou seconde extrémité étant identifiée par une adresse IP, un port et un protocole de transport, chaque connexion étant identifiée par un jeu de paramètres {IPa, Pa, IPb, Pb, proto} correspondant respectivement à l'adresse IP et au port de la première extrémité, à l'adresse IP et au port de la seconde extrémité, et au protocole de transport commun aux
30 première et seconde extrémités,

lesdites premières et secondes étapes de conversion d'adresse comprennent, pour chaque paquet, les étapes suivantes :

- lecture des champs "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet, de façon à disposer d'un jeu de paramètres correspondant aux contenus desdits champs lus et permettant d'identifier une connexion d'origine empruntée par ledit paquet ;
- recherche dans une table de conversion d'une entrée correspondant à ladite connexion d'origine empruntée par le paquet, ladite table de conversion associant une connexion transposée distincte à chaque connexion d'origine ;
- s'il n'existe pas d'entrée correspondant à ladite connexion d'origine empruntée par le paquet, création et ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) ;
- modification dudit paquet, de façon à remplacer la connexion d'origine par la connexion transposée qui lui est associée.

De cette façon, l'adresse IP normalisée de l'ensemble du réseau privé est partagée dans le temps par différentes connexions, chaque connexion étant définie par un jeu de cinq paramètres. Ainsi, pour chaque paquet (sortant ou entrant) à traiter, on détermine la connexion d'origine utilisée par ce paquet, et à partir d'une table de conversion, on en déduit une connexion transposée que doit utiliser le paquet pour la suite de son trajet.

Une connexion TCP/IP s'établit entre deux couples (adresse IP source/port source) et (adresse IP destination/port destination). D'un point de vue plus applicatif, une connexion s'établit toujours suivant un principe client/serveur. C'est-à-dire qu'une application désirant dialoguer avec un service va établir une communication avec la machine supportant ce service (ce qui définit l'adresse IP destination). Cette machine pouvant supporter différentes applications, c'est le port destination qui va permettre de sélectionner l'application souhaitée.

Si le paquet est sortant, les deux adresses IP source et destination de la connexion transposée sont des adresses IP normalisées. Si le paquet est entrant, les deux adresses IP source et destination de la connexion d'origine sont des adresses IP normalisées.

Dans un premier mode de réalisation avantageux du procédé de l'invention, ladite

étape de création et d'ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) consiste à créer dans ladite table de conversion une première et une seconde entrée associant chacune un jeu de paramètres d'origine $J_o = \{ip_src, p_src, ip_dst, p_dst, p_proto\}$ à un jeu de paramètres transposés $J_t = \{ip_src', p_src', ip_dst', p_dst', p_proto'\}$,

et, lorsque ladite connexion d'origine est sortante, c'est-à-dire initiée par ladite première extrémité du premier réseau, lesdits jeux de paramètres d'origine et transposés s'écrivent respectivement :

- pour ladite première entrée : $J_{o,1} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,1} = \{IPv, Pv, IPb, Pb, proto\}$,
- pour ladite seconde entrée : $J_{o,2} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,2} = \{IPb, Pb, IPa, Pa, proto\}$,

les paramètres IPa, Pa, IPb, Pb et $proto$ étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

les paramètres IPv, Pv et $proto$ définissant une extrémité virtuelle, IPv étant ladite adresse IP normalisée intermédiaire et unique, et Pv étant un port dont la valeur est calculée en dynamique, de façon qu'il n'existe aucune autre connexion de la table de conversion possédant le même couple (IPv, Pv).

Toutes les extrémités virtuelles ($IPv, Pv, proto$) possèdent une même adresse IP normalisée : c'est l'adresse unique (IPv) du réseau privé dans le réseau normalisé. En revanche, elles se distinguent les unes des autres par la valeur des deux autres paramètres, à savoir le port et le protocole.

Préférentiellement, dans ce premier mode de réalisation, lorsque ladite connexion d'origine est entrante, c'est-à-dire initiée par ladite seconde extrémité du second réseau, lesdits jeux de paramètres d'origine et transposés s'écrivent respectivement :

- pour ladite première entrée : $J_{o,1} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,1} = \{IPb, Pb, IPa, Pa, proto\}$,
- pour ladite seconde entrée : $J_{o,2} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,2} = \{IPv, Pv, IPb, Pb, proto\}$,

les paramètres IPb, Pb, IPv, Pv et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

les paramètres IPv, Pv et proto définissant une extrémité virtuelle, IPv étant ladite adresse
5 IP normalisée intermédiaire et unique, ou bien, au choix de l'administrateur, une adresse IP choisie dans la plage d'adresses normalisées attribuée au site à connecter, et Pv étant un port prédéterminé,

et le couple de paramètres (IPa, Pa) étant trouvé, grâce au couple de paramètres (IPv, Pv), par lecture d'une table de correspondance statique associant de façon bijective à
10 chaque couple de paramètres (IPa, Pa) parmi une pluralité prédéterminée un couple de paramètres (IPv, Pv) distinct.

Dans un second mode de réalisation avantageux du procédé de l'invention, ladite étape de création et d'ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) consiste à créer dans ladite table de
15 conversion une unique entrée associée à un jeu combiné de paramètres d'origine et transposés $J_c = \{ip_0, p_0, ip_1, p_1, ip_2, p_2, \text{proto}\}$,

et, lorsque ladite connexion d'origine est sortante, c'est-à-dire initiée par ladite première extrémité du premier réseau, ledit jeu combiné de paramètres d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, \text{proto}\}$,

20 les paramètres IPa, Pa, IPb, Pb et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

les paramètres IPv, Pv et proto définissant une extrémité virtuelle, IPv étant ladite adresse IP normalisée intermédiaire et unique, et Pv étant un port dont la valeur est calculée en
25 dynamique, de façon qu'il n'existe aucune autre connexion de la table de conversion possédant le même couple (IPv, Pv).

Le calcul du paramètre Pv est dynamique et ne peut avoir lieu que sur des connexions sortantes.

Préférentiellement, lorsque ladite connexion d'origine est entrante, c'est-à-dire
30 initiée par ladite seconde extrémité du second réseau, ledit jeu combiné de paramètres

d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, proto\}$,
les paramètres IPb, Pb, IPv, Pv et $proto$ étant lus dans les champs respectivement
"adresse IP source", "port source", "adresse IP destination", "port destination", et
"protocole de transport" dudit paquet, ou bien, au choix de l'administrateur, une adresse
5 IP choisie dans la plage d'adresses normalisées attribuée au site à connecter.

les paramètres IPv, Pv et $proto$ définissant une extrémité virtuelle, IPv étant ladite adresse
IP normalisée intermédiaire et unique, et Pv étant un port prédéterminé,
et le couple de paramètres (IPa, Pa) étant trouvé, grâce au couple de paramètres (IPv, Pv) ,
par lecture d'une table de correspondance statique associant de façon bijective à
10 chaque couple de paramètres (IPa, Pa) parmi une pluralité prédéterminée un couple de
paramètres (IPv, Pv) distinct.

Ainsi, il est possible, pour les connexions entrantes, d'effectuer une conversion
"statique", la recherche du couple de paramètres (Ipa, Pa) étant effectuée parmi un
ensemble de couple prédéterminé.

15 Avantageusement, dans le cas du premier mode de réalisation, pour chaque
paquet sortant, ladite étape de modification du paquet consiste à remplacer le contenu des
champs "adresse IP source" et "port source" du paquet par les paramètres correspondants
 ip_src' et p_src' dudit jeu de paramètres transposés J_i d'identification de la connexion
transposée,

20 et, pour chaque paquet entrant, ladite étape de modification du paquet consiste à
remplacer le contenu des champs "adresse IP destination" et "port destination" du paquet
par les paramètres correspondants ip_dst' et p_dst' dudit jeu de paramètres transposés J_i
d'identification de la connexion transposée.

Ainsi, vu de la première extrémité du premier réseau, il existe une connexion entre
25 cette première extrémité et la seconde extrémité du second réseau. En revanche, vu de la
seconde extrémité du second réseau, il existe une connexion entre cette seconde extrémité
et une extrémité virtuelle du second réseau (et non pas la première extrémité du premier
réseau).

30 Avantageusement, dans le cas du second mode de réalisation, pour chaque paquet
sortant, ladite étape de modification du paquet consiste à remplacer le contenu des champs

“adresse IP source” et “port source” du paquet par les paramètres ip_2 et p_2 dudit jeu combiné de paramètres d’origine et transposés J_c ,

et, pour chaque paquet entrant, ladite étape de modification du paquet consiste à remplacer le contenu des champs “adresse IP destination” et “port destination” du paquet par les paramètres ip_0 et p_0 dudit jeu combiné de paramètres d’origine et transposés J_c .

Préférentiellement, ladite table de conversion est mise à jour de façon dynamique selon une stratégie prédéterminée de mise à jour. Ainsi, la taille mémoire de la table de conversion peut être limitée et l’étape de recherche d’une connexion d’origine dans la table, si elle existe, peut être effectuée plus rapidement.

Plusieurs stratégies de mise à jour peuvent être envisagées.

Dans un mode de réalisation avantageux de l’invention, ladite stratégie prédéterminée de mise à jour consiste à ne laisser chaque couple de connexions d’origine et transposée inscrit dans la table de conversion qu’entre un instant de début et un instant de fin de vie de ladite connexion d’origine. En d’autres termes, une connexion est ôtée de la table de conversion dès que sa durée de vie s’est écoulée.

De façon avantageuse, dans le cas d’une connexion utilisant le protocole TCP, lesdits instants de début et de fin de vie de la connexion d’origine sont déterminés en se référant au diagramme d’état d’une session TCP, selon la spécification TCP (RFC 793).

Avantageusement, dans le cas d’une connexion utilisant le protocole UDP, ledit instant de début de vie de la connexion d’origine est déterminé par le passage, dans un sens donné, d’un paquet de requête, et en ce que ledit instant de fin de vie est déterminé par le passage, dans le sens inverse dudit sens donné, d’un paquet de réponse.

Ainsi, même si cela peut sembler contradictoire avec le principe même d’UDP, on introduit selon l’invention une notion de connexion UDP. En effet, le protocole UDP est par principe “non connecté”.

En fait, une analyse des applications utilisant le protocole UDP permet de les classer en deux grandes catégories :

- les applications utilisant la diffusion multiple (broadcast en anglo-saxon). Ces applications n’ont en général qu’une utilité locale. Elles peuvent donc être supprimées sans inconvénient au niveau d’un dispositif de

raccordement inter-réseaux ;

- les applications du type requête/réponse. Un paquet UDP est émis vers une machine et un port particulier et contient une requête. A la destination se trouve un serveur qui analyse le paquet reçu et renvoie une réponse, elle-même encapsulée dans un paquet UDP. Quelques exemples d'applications de ce type : Serveur d'horloge, Serveur de noms (DNS)...

5

Ce dernier type d'application permet de retrouver l'idée de connexion. Au niveau d'un dispositif de raccordement inter-réseaux, une connexion commence d'exister lorsque passe un paquet UDP n'appartenant à aucune connexion repérée et se termine lorsque passe en sens inverse un paquet de réponse.

10

Comme le principe de l'invention consiste à appliquer une translation d'adresses à chaque connexion, le fait de définir des "connexions UDP" permet de rendre le procédé de l'invention applicable au protocole UDP.

15

Selon une variante avantageuse, dans le cas d'une connexion utilisant le protocole UDP, ledit instant de début de vie de la connexion d'origine est déterminé par le passage, dans un sens donné, d'un paquet de requête, et en ce que ledit instant de fin de vie est déterminé par l'écoulement d'une durée prédéterminée depuis ledit instant de début de vie.

20

Afin de supporter un maximum d'applications présentes et futures, on peut affiner ce mécanisme de détection des connexions en offrant une possibilité de paramétrage par l'utilisateur de ce qui va déterminer la fin de la connexion : un ou plusieurs paquets de réponse, ou bien l'expiration d'une temporisation armée par la requête. De même, il est possible de paramétrer la possibilité d'avoir plusieurs requêtes au travers de la même connexion. Tous ces paramétrages peuvent bien sûr être définissables en fonction de l'application (déterminée par le port destination du paquet initialisant la connexion).

25

Dans un mode de réalisation préférentiel de l'invention, le procédé comprend une étape de filtrage des paquets sortants en fonction du contenu d'un des champs appartenant au groupe comprenant les champs "adresse IP source", "adresse IP destination" et "port destination".

30

L'invention concerne également un dispositif d'interconnexion de réseaux mettant

chacun en oeuvre la technologie internet, du type destiné à être inséré entre un premier réseau présentant un adressage IP privé et un second réseau présentant un adressage IP normalisé, lesdits premier et second réseaux véhiculant des paquets, chacun desdits paquets comportant un en-tête IP comprenant notamment un champ "adresse IP source" et un champ "adresse IP destination", les paquets étant dits sortants s'ils se déplacent du premier vers le second réseau à travers ledit dispositif et entrants dans le cas contraire,

ledit dispositif possédant une adresse IP normalisée intermédiaire et unique dans ledit second réseau, et comprenant notamment :

- des premiers moyens de conversion des adresses IP privées contenues dans les champs "adresse IP source" des paquets sortants, de façon que ledit champ "adresse IP source" de chacun desdits paquets sortants contienne, après conversion, ladite adresse IP normalisée intermédiaire et unique ; et
- des seconds moyens de conversion de l'adresse IP normalisée intermédiaire et unique contenue dans les champs "adresse IP destination" des paquets entrants, de façon que ledit champ "adresse IP destination" de chacun desdits paquets entrants contienne, après conversion, une des adresses privées du premier réseau.

Avantageusement, chacun desdits paquets comportant un en-tête TCP ou UDP comprenant notamment un champ "port source" et un champ "port destination", ledit en-tête IP comprenant en outre un champ "protocole de transport" indiquant le protocole TCP ou UDP utilisé,

lesdits premiers et seconds moyens de conversion d'adresse comprennent :

- des moyens de réception et de stockage d'un paquet ;
- des moyens de lecture d'un paquet reçu et stocké, permettant d'identifier une connexion d'origine empruntée par ledit paquet, par la connaissance d'un jeu de paramètres d'identification qui sont les contenus des champs "adresse IP source", "adresse IP destination", "port source", "port destination", et "protocole de transport" du paquet reçu et stocké ;
- au moins une table de conversion, associant une connexion transposée distincte à chaque connexion d'origine, chacune desdites connexion d'origine ou transposée étant identifiée par un jeu distinct de paramètres d'identification ;

- des moyens de lecture de ladite table de transposition, permettant de lire le jeu de paramètres d'identification de la connexion transposée associée à la connexion d'origine empruntée par le paquet reçu et stocké ;
- des moyens de modification dudit paquet reçu et stocké permettant de substituer le jeu de paramètres d'identification de la connexion transposée au jeu de paramètres d'identification contenus dans le paquet reçu et stocké, de façon à remplacer la connexion d'origine par la connexion transposée qui lui est associée dans la table de conversion.

L'invention concerne aussi un routeur IP d'interconnexion de réseaux, caractérisé en ce qu'il comprend un dispositif présentant les caractéristiques précitées, ladite adresse IP normalisée intermédiaire et unique étant l'adresse IP normalisée de raccordement dudit routeur IP audit second réseau.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation préférentiel de l'invention, donnée à titre d'exemple indicatif et non limitatif, et des dessins annexés, dans lesquels :

- la figure 1 illustre le principe général du procédé d'interconnexion de réseaux selon l'invention ;
- la figure 2 présente la structure connue d'un paquet TCP/IP ;
- la figure 3 présente la structure connue d'un en-tête IP ;
- la figure 4 présente la structure connue d'un en-tête TCP ;
- la figure 5 présente la structure connue d'un en-tête UDP ;
- la figure 6 illustre une transposition de connexion telle que réalisée par le procédé de l'invention ;
- la figure 7 présente un organigramme d'un mode de réalisation particulier du procédé de l'invention ;
- les figures 8 et 9 présentent chacune en détail l'une des étapes de l'organigramme de la figure 7 ;
- la figure 10 est un schéma synoptique simplifié d'un dispositif d'interconnexion de réseaux selon l'invention ;
- la figure 11 est un exemple de réalisation de la table de connexion comprise dans le dispositif de la figure 10 ; et

- la figure 12 illustre un exemple d'application du procédé et du dispositif de l'invention.

L'invention concerne donc un procédé et un dispositif d'interconnexion de deux réseaux mettant chacun en oeuvre la technologie internet (ou technologie TCP/IP).

5 Comme illustré sur la figure 1, il s'agit d'interconnecter :

- un premier réseau 1 présentant un adressage IP privé ; et
- un second réseau 2 présentant un adressage IP normalisé.

L'interconnexion des deux réseaux 1, 2 consiste notamment à effectuer une conversion d'adresse 3.

10 Le second réseau 2 est par exemple le réseau mondial Internet. Le premier réseau 1 est par exemple un réseau local d'entreprise dont l'adressage a été défini en dehors de l'autorité globale pour l'attribution des adresses.

Le terme "privé" qualifiant l'adressage IP du premier réseau 1 s'entend ici comme l'inverse de "normalisé".

15 La technologie connue internet est basée sur une suite de protocoles dont les plus importants sont IP, TCP et UDP.

Le protocole IP (pour Internet Protocol en anglo-saxon) est le protocole de base de la technologie internet. Il a pour simple fonction de transférer un paquet de données (c'est-à-dire un ensemble d'octets) d'une machine à une autre.

20 Le protocole TCP (pour Transmission Control Protocol en anglo-saxon) s'appuie sur le protocole IP et a pour objet d'assurer une communication en mode connecté, c'est-à-dire d'assurer un circuit virtuel entre deux applications situées sur des machines distinctes. Pour cela, le protocole TCP doit assurer la fiabilité des transmissions, l'ordonnancement et le contrôle de flux. Le flux de données envoyé par une application
25 est donc segmenté en paquets. A chacun de ces paquets est ajouté un en-tête TCP (dont la structure est présentée sur la figure 4). Chaque paquet ainsi complété est ensuite confié au protocole IP qui y ajoute son propre en-tête IP (dont la structure est présentée sur la figure 3).

30 Le protocole UDP (pour User Datagram Protocol en anglo-saxon) s'appuie également sur le protocole IP et a pour objet d'assurer une communication en mode non

connecté. Le choix du protocole UDP correspond aux applications reposant sur un trafic faible ou sur des échanges du type "question-réponse".

Le protocole UDP ajoute un en-tête (dont la structure est présentée sur la figure 5) aux données à transmettre. Ce paquet est ensuite confié au protocole IP qui y ajoute son propre en-tête IP.

Les paquets ont donc construits selon un principe d'encapsulations successives :

- on ajoute aux données un en-tête TCP ou UDP, de façon à former un paquet TCP ou UDP ; puis
- on ajoute au paquet TCP ou UDP un en-tête IP.

La figure 2 présente la structure connue d'un paquet TCP/IP 21. La structure connue d'un paquet UDP/IP se déduit facilement de la précédente par remplacement de l'en-tête TCP par un en-tête UDP.

L'en-tête IP 31 dont la structure connue est présentée sur la figure 3, comprend notamment :

- un champ "protocole" 32 définissant le protocole utilisé, par exemple TCP ou UDP. En effet, les données que véhicule un paquet IP sont en fait des unités de protocole d'un niveau supérieur (principe d'encapsulation) ;
- un champ "adresse IP source" 33 et un champ "adresse IP destination" 34 définissant l'adresse IP émettrice et l'adresse IP de la machine destinatrice respectivement.

Le protocole IP permet d'envoyer des données d'une machine à une autre. Comme ces machines sont généralement multi-application, il est nécessaire de fournir un moyen d'identifier les applications qui désirent communiquer entre elles. Ceci est fait par les protocoles TCP et UDP, en introduisant la notion de "port". En effet, les en-têtes TCP 41 et UDP 51, dont les structures connues sont présentées sur les figures 4 et 5 respectivement, comprennent notamment un champ "port source" 42, 52 et un champ "port destination" 43, 53.

Le champ "port destination" 43, 53 permet de sélectionner l'application souhaitée parmi celles supportées par la machine destinatrice, c'est-à-dire celle dont l'adresse IP est définie par le champ "adresse IP destination" 34 de l'en-tête IP 31.

Le procédé d'interconnexion de réseaux de l'invention est basé sur une analyse des connexions utilisées par les paquets. Selon l'invention, la notion de connexion, qui s'applique généralement uniquement au protocole TCP, est généralisée de façon à s'appliquer également au protocole UDP.

5 On appelle extrémité de réseau une entité logicielle (par exemple une application) pouvant être décrite par les trois paramètres suivants : une adresse IP, un port et un protocole (TCP ou UDP).

 On appelle connexion un lien logique entre deux extrémités de réseau, l'une étant cliente et l'autre serveur. Une extrémité peut faire partie de plusieurs connexions
10 différentes. Une fois initiée, une connexion est un chemin de communication permettant des échanges de données bidirectionnels.

La connexion entre les deux extrémités $A = \{IPa, Pa, proto\}$ et $B = \{IPb, Pb, proto\}$ peut être désignée, de façon unique par les cinq paramètres suivants :

- IPa : l'adresse IP de la première extrémité A ;
- 15 - IPb : l'adresse IP de la seconde extrémité B ;
- Pa : le port de la première extrémité A ;
- Pb : le port de la seconde extrémité B ;
- proto : le protocole de la connexion (TCP ou UDP).

20 Par la suite, on note la connexion C_{AB} de la façon suivante : $C_{AB} = \{IPa, Pa, IPb, Pb, proto\}$.

On considère dans la suite de la description que l'extrémité $A = \{IPa, Pa, proto\}$ est située dans le premier réseau 1 à adressage IP privé et que l'extrémité $B = \{IPb, Pb, proto\}$ est située dans le second réseau 2 à adressage IP normalisé. En d'autres termes, l'adresse IPa est une adresse privée alors que l'adresse IPb est une adresse normalisée.

25 On appelle paquets sortants les paquets se déplaçant du premier réseau 1 vers le second réseau 2, et paquets entrants les paquets se déplaçant dans le sens inverse.

Le principe général de l'invention est de modifier les paquets transmis entre les premier et second réseaux 1, 2, de façon que :

- pour chaque paquet sortant, l'adresse IP privée contenue dans le champ
30 "adresse IP source" 33 soit remplacée par une adresse IP normalisée

intermédiaire et unique, notée IPv (à noter que le principe défini ici est vrai pour les connexions sortantes. Pour les connexions entrantes, IPv n'est pas forcément unique) ;

- pour chaque paquet entrant, l'adresse IPv contenue dans le champ "adresse IP destination" soit remplacée par l'adresse IP privée adéquate.

Ainsi, après modification, tous les paquets sortants possèdent une même adresse IP source, à savoir IPv. De même, avant modification, tous les paquets entrants possèdent une même adresse IP destination, à savoir IPv. Par conséquent, une seule adresse IP normalisée suffit pour raccorder tout le premier réseau 1 à adressage privé au second réseau 2 à adressage normalisé.

En termes de connexions, le procédé de l'invention consiste à déporter l'extrémité A de la connexion C_{AB} sur une extrémité virtuelle V. En d'autres termes, comme illustré sur la figure 6, on réalise au point V une transposition de la connexion C_{AB} en une connexion virtuelle C_{VB} . La transposition de C_{AB} en C_{VB} est effectuée :

- pour les paquets sortants, en remplaçant les paramètres source IPa et Pa de C_{AB} par les paramètres source IPv et Pv de C_{VB} ;
- pour les paquets entrants, en remplaçant les paramètres destination IPv et Pv de C_{VB} par les paramètres destination IPa et Pa de C_{AB} .

Le fonctionnement du procédé de l'invention repose sur le maintien d'une table de conversion, associant à chaque connexion d'origine utilisée sa connexion transposée.

Le fonctionnement d'un mode de réalisation particulier du procédé de l'invention est maintenant présenté en relation avec les organigrammes des figure 7, 8 et 9.

L'organigramme de la figure 7 présente l'ensemble du traitement (70) effectué sur chaque paquet.

Tout d'abord, on vérifie (71) que les totaux de contrôle 34, 44, 54 (ou checksums, en anglo-saxon) des en-têtes IP et TCP ou UDP (cf figure 3, 4, et 5) sont corrects. S'ils ne le sont pas, le paquet est éliminé (72). Sinon, les paramètres { ip_src, p_src, ip_dst, p_dst, proto } sont extraits (73) du paquet, de façon à identifier la connexion d'origine C correspondant à ces paramètres.

On cherche ensuite (74) s'il existe une entrée de la table de conversion

correspondant à cette conversion d'origine C. S'il n'en existe pas, on regarde (75) si le paquet est cohérent et peut-être un début de connexion d'origine. Si c'est le cas, l'enregistrement (76) de cette connexion d'origine et de sa connexion transposée associée est effectué (cf explication détaillée par la suite, en relation avec la figure 8). Si ce n'est pas le cas, le paquet est éliminé (72).

Après enregistrement (76) ou si la connexion d'origine était déjà enregistrée (c'est-à-dire s'il existe une entrée correspondante), le paquet est modifié (77) (cf explication détaillée par la suite, en relation avec la figure 9), puis le paquet est acheminé (78).

Enfin, si la connexion d'origine est terminée (79), les deux entrées correspondant à cette connexion d'origine sont ôtées (710) de la table des connexions.

On explique maintenant en détail, en relation avec la figure 8, l'étape 76 d'enregistrement de la connexion d'origine et de sa connexion transposée associée.

Cette étape (76) consiste à créer dans ladite table de conversion une première et une seconde entrée associant chacune un jeu de paramètres d'origine $J_o = \{ip_src, p_src, ip_dst, p_dst, p_proto\}$ à un jeu de paramètres transposés $J_t = \{ip_src', p_src', ip_dst', p_dst', p_proto'\}$.

On distingue deux cas, selon que la connexion d'origine est entrante, c'est-à-dire initiée par une extrémité (A par exemple dans la suite de la description) du premier réseau 1, ou sortante, c'est-à-dire initiée par une extrémité (B par exemple dans la suite de la description) du second réseau 2.

Si la connexion d'origine est sortante, par exemple de A vers B, on effectue les étapes suivantes :

- calcul (83) de IPV et PV pour former C_{VB} ;
- enregistrement (84) d'une première et d'une seconde entrées associant les jeux de paramètres d'origine et transposés suivants :
 - * pour ladite première entrée :
 $J_{o,1} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,1} = \{IPv, Pv, IPb, Pb, proto\}$,
 - * pour ladite seconde entrée :
 $J_{o,2} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,2} = \{IPb, Pb, IPa, Pa, proto\}$.

Ces quatre jeux de paramètres $J_{o,1}$, $J_{t,1}$, $J_{o,2}$ et $J_{t,2}$ sont illustrés sur la figure 11 qui présente un mode de réalisation particulier d'une table de conversion utilisée dans la mise en oeuvre du procédé de l'invention.

La seconde entrée est destinée à être utilisée lors du traitement des paquets de retour.

Les paramètres IPa, Pa, IPb, Pb et proto sont lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" du paquet.

Les paramètres IPv, Pv et proto définissent une extrémité virtuelle V, IPv étant l'adresse IP normalisée intermédiaire et unique. La valeur du port Pv est calculée (83) en dynamique, de façon qu'il n'existe aucune autre connexion de la table de conversion possédant le même couple (IPv, Pv).

Si la connexion d'origine est entrante, par exemple de B vers V, on effectue les étapes suivantes :

- recherche (82) de IPa et Pa, si le couple (IPv, Pv) est tel qu'il existe une extrémité A déportée (par exemple une application donnée sur un serveur déporté du réseau privé) (81) ;
- enregistrement (84) d'une première et d'une seconde entrées associant les jeux de paramètres d'origine et transposés suivants :
 - * pour ladite première entrée :
 $J_{o,1} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,1} = \{IPb, Pb, IPa, Pa, proto\}$,
 - * pour ladite seconde entrée :
 $J_{o,2} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,2} = \{IPv, Pv, IPb, Pb, proto\}$.

La seconde entrée est destinée à être utilisée lors du traitement des paquets de retour.

Les paramètres IPv, Pv et proto définissent une extrémité virtuelle V, IPv étant l'adresse IP normalisée intermédiaire et unique, ou bien, au choix de l'administrateur, une adresse IP choisie dans la plage d'adresses normalisées attribuée au site à connecter, et Pv étant un port prédéterminé.

Le couple de paramètres (IPa, Pa) est trouvé (82), grâce au couple de paramètres

(IPv, Pv), par lecture d'une table de correspondance statique associant de façon bijective à chaque couple de paramètres (IPa, Pa) parmi une pluralité prédéterminée un couple de paramètres (IPv, Pv) distinct.

5 Il est à noter que dans une mode de réalisation simplifié du procédé de l'invention, les connexions entrantes sont rejetées par principe. Ainsi, grâce au connexions sortantes, les machines du réseau privé 1 ont accès aux ressources disponibles, sur le réseau normalisé 2, mais les machines du réseau normalisé 2 n'ont pas accès aux "ressources" du réseau privé 1 (dissymétrie du principe de translation d'adresse).

10 On explique maintenant en détail, en relation avec la figure 9, l'étape 77 de modification du paquet.

On examine (91) le protocole de a connexion d'origine, de façon à savoir si celle-ci se termine. Si elle se termine, on arme (92) un temporisateur de libération de connexion (on libère alors les entrées correspondant à cette connexion d'origine) et créés
15 simultanément (cf figure 8)). Après cet armement (92) ou si la connexion d'origine ne se termine pas, on effectue les modifications.

Pour effectuer ces modifications, on distingue deux cas, selon que le paquet est sortant ou entrant.

20 Si le paquet est sortant, la transposition de connexion est réalisée au remplaçant (93), dans le champ "adresse Ip source" du paquet, IPa par IPv, et dans le champ "port source" du paquet, Pa par Pv.

Si le paquet est entrant, la transposition de connexion est réalisée en remplaçant (94), dans le champ "adresse IP destination" du paquet , IPv par IPa, et dans le champ "port destination" du paquet, Pv par Pa.

25 Le paquet ainsi modifié subit une étape 95 de "traitement particulier connexion", consistant à gérer les particularités liées à certains protocoles applicatifs, comme FTP, rep et rch. Ces particularités et leur traitement sont définies plus loin dans ce document.

Enfin, les totaux de contrôle (checksums) des en-têtes IP et TCP ou UDP sont recalculés (96).

30 Dans le premier mode de réalisation du procédé de l'invention présenté ci-dessus,

pour chaque couple (connexion d'origine, connexion transposée), on crée deux entrées dans la table (une pour chaque sens de paquet) et le traitement, du point de vue lecture dans la table, est identique pour les paquets sortants et la paquets entrants.

5 On présente maintenant un second mode de réalisation du procédé de l'invention, dans lequel, pour chaque couple (connexion d'origine, connexion transposée), on crée une seule entrée dans la table et le traitement, du point de vue lecture dans la table, est différent selon que les paquets sont sortants ou entrants.

10 Dans ce second mode de réalisation, l'étape de création et d'ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) consiste à créer dans la table de conversion une unique entrée associée à un jeu combiné de paramètres d'origine et transposés $J_c = \{ip_0, p_0, ip_1, p_1, ip_2, p_2, proto\}$.

15 Lorsque ladite connexion d'origine est sortante, le jeu combiné de paramètres d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, proto\}$. Les paramètres IPa, Pa, IPb, Pb et $proto$ sont lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" du paquet. Les paramètres IPv, Pv et $proto$ définissent une extrémité virtuelle V , IPv étant l'adresse IP normalisée intermédiaire et unique et Pv étant un port dont la valeur est calculée en dynamique.

20 Lorsque la connexion d'origine est entrante, le jeu combiné de paramètres d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, proto\}$. Les paramètres IPb, Pb, IPv, Pv et $proto$ sont lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" du paquet. Les paramètres IPv, Pv et $proto$ définissent une extrémité virtuelle V , IPv étant l'adresse IP normalisée intermédiaire et unique, ou bien, au choix de l'administrateur, 25 une adresse IP choisie dans la plage d'adresses normalisées attribuée au site à connecter, et Pv étant un port prédéterminé. Le couple de paramètres (IPa, Pa) étant trouvé associé de façon statique à un couple prédéterminé de paramètres (IPv, Pv) distinct.

30 Dans ce second mode de réalisation, pour chaque paquet sortant, l'étape de modification du paquet consiste à remplacer le contenu des champs "adresse IP source" et "port source" du paquet par les paramètres ip_2 et p_2 du jeu combiné de paramètres

d'origine et transposés J_c . Pour chaque paquet entrant, l'étape de modification du paquet consiste à remplacer le contenu des champs "adresse IP destination" et "port destination" du paquet par les paramètres ip_0 et p_0 du jeu combiné de paramètres d'origine et transposés J_c .

- 5 D'une façon générale, une connexion peut être :
- soit utilisée, si au moins un paquet cohérent a été échangé entre les deux extrémités et si l'on ne peut pas assurer qu'il ne passera plus d'autre paquet cohérent pour cette connexion ;
 - soit libre, si aucun paquet n'a transité entre les deux extrémités.

10 Le fonctionnement des deux modes de réalisation du procédé de l'invention présentés ci-dessus repose sur le maintien d'une table des connexions utilisée (c'est-à-dire sur la suppression des connexions qui redeviennent libres). Il faut donc déterminer les instants de début et de fin de vie de chaque connexion enregistrée dans la table de conversion.

15 Pour les connexions dont le protocole est TCP, ces instants de début et de fin de vie de la connexion sont par exemple déterminés en se référant au diagramme d'état d'une session TCP, selon la spécification TCP (RFC 793). On se basera notamment sur le champ "drapeaux" de l'en-tête TCP et particulièrement sur les bits SYN pour le début de la connexion et FIN pour la fin de celle-ci. On pourra prévoir aussi un temporisateur de sécurité, armé par le passage d'un paquet avec le bit FIN et supprimant la connexion au bout d'un certain temps d'inactivité, ceci pour résoudre le cas d'une déconnexion initiée, mais non parvenue à terme, cas possible, par exemple, avec une extrémité devenue inactive, donc incapable de participer à la clôture de la connexion.

20 Pour les connexions dont le protocole est UDP, on peut définir l'instant de début de vie de la connexion par le passage, dans un sens donné, d'un paquet de requête, et l'instant de fin de vie de la connexion par le passage, dans l'autre sens, d'un paquet de réponse.

25 Selon une variante, on définit l'instant de fin de vie par écoulement d'une durée prédéterminée depuis l'instant de début de vie.

30 On peut imaginer d'autres variantes selon lesquelles l'instant de fin de vie de la

connexion, dans le cas UDP, est fonction de différents critères (nombre de paquets, expiration d'une durée prédéterminée,...), ces critères étant bien sûr paramétrables par type de connexion.

Dans un mode de réalisation particulier, on peut s'affranchir de la nécessité de déterminer le début et la fin de connexion en utilisant le principe suivant :

- une connexion est créée lorsque apparaît un nouveau paquet n'appartenant à aucune connexion existante ;
- on maintient constamment une variable définissant l'heure du dernier paquet ayant transité sur cette connexion ;
- la fin de la connexion n'étant pas détectée, celle-ci restera dans la table alors qu'elle n'a plus d'existence ;
- le numéro de port garantissant l'unicité étant codé sur 2 octets, soit 65535 valeurs possibles, la table va théoriquement arriver à saturation lorsque 65535 connexions auront été effectuées,
- on procédera alors à la suppression de la table de l'entrée correspondant à la connexion dont la variable notant l'heure du dernier paquet est la plus ancienne.

En pratique, afin de limiter l'occupation mémoire, on procédera à cette suppression à partir d'un nombre de connexions simultanées défini par l'administrateur du système.

Optionnellement, le traitement de chaque paquet peut comprendre une étape de filtrage des paquets, en fonction du contenu d'au moins un des champs suivants : "adresse IP source", "adresse IP destination" et "port destination". Ainsi, on peut limiter le nombre de station du réseau privé 1 ayant accès au réseau normalisé 2, ou bien limiter cet accès à certaines applications.

La figure 12 illustre un exemple d'application du procédé de l'invention.

Si on considère que l'extrémité A est sur un réseau privé R1, que l'extrémité B est sur un réseau "normalisé" R2, par exemple Internet, et que le point V est sur un canal de passage incontournable entre les deux réseaux R1 et R2, on réalise l'application recherchée de l'invention : on rend possible une connexion d'un site privé avec un site

d'un réseau normalisé, sans modifier les adresses du réseau privé.

En référence à la figure 12, l'extrémité A est par exemple un client telnet sur la machine M1 : $A = \{IPm1, Pn, TCP\}$; où IPm1 est l'adresse IP de la machine M1, Pn est un port client déterminé de la machine M1, et TCP est le protocole TCP. L'extrémité B est par exemple un serveur telnet de la machine M2 : $B = \{IPm2, 23, TCP\}$; 23 étant le port connu TCP du serveur telnet. Le tout forme la connexion $C = \{IPm1, Pn, IPm2, 23, TCP\}$.

Le réseau R1 est un réseau privé dont les routes par défaut vont vers le réseau R2. Le réseau R2 ne connaît pas l'existence de R1. Le procédé de l'invention est mis en oeuvre dans la machine ou passerelle P. Cette passerelle P est connectée aux deux réseaux, à l'adresse privée IPr1 pour R1, à l'adresse normalisée IPr2 pour R2.

Dans ces conditions, la connexion C ne peut fonctionner, car les paquets circulent bien dans le sens M1 vers M2, mais ne peuvent pas revenir vers M1 car le réseau R1 est inconnu des machines situées vers le réseau R2.

Si la passerelle P exploite le procédé de l'invention, on peut transposer au point V la connexion C en une connexion C2 en remplaçant l'extrémité A par une extrémité virtuelle VA telle que VA soit sur le réseau R2 et que C2 transite par le point V. Pour satisfaire cette condition, la solution est de substituer IPm1 par IPr2 dans les paquets transitant par la passerelle P. Donc on peut transposer C en $C2 = \{IPr2, Pn, IPm2, 23, TCP\}$. Le procédé requiert également que C2 soit libre, c'est-à-dire qu'au point V, on aura pris soin de noter toutes les connexions qui y transitent, de façon à vérifier qu'il n'y ait pas de client telnet avec le même port Pn vers la même destination (extrémité B). Si cela était le cas, on transformerait VA en $\{IPr2, Pm, TCP\}$, Pm étant un port TCP inutilisé de la passerelle P.

La translation des adresses et des ports dans les paquets IP est généralement transparente pour les applications TCP/IP. Seules trois applications particulières nécessitent un traitement spécifique, à savoir FTP (pour File Transfer Protocol en anglo-saxon), RCP (pour Remote copy (Transfert de fichiers) en anglo-saxon) et RSH (pour Remote Shell (Exécution à distance) en anglo-saxon).

L'application FTP permet le transfert de fichier d'une machine à une autre. Le

protocole FTP est défini selon la spécification TCP, par le RFC 959. Ce protocole offre la particularité d'utiliser par session utilisateur une connexion TCP pour les commandes et d'y ajouter une autre connexion TCP pour les données du fichier en cours de transfert.

5 Cette autre connexion, pour les données, est établie par le serveur. Donc, elle apparaît comme connexion entrante pour le dispositif mettant en oeuvre le procédé de l'invention, qui, par défaut, refuse ce type de connexion.

Une solution est donc de détecter les connexions de commande FTP. Ce qui se fait en examinant le port destination qui, pour cette application est fixé à 21. A chaque connexion de commande FTP, on va donc adjoindre une entrée dans la table de conversion d'origine. Cette conversion va être déterminée en examinant les commandes transitant sur le canal. Le client FTP envoie une commande PORT ayant pour paramètre l'adresse IP et le numéro de port sur lequel doit être établie la connexion. Ces paramètres doivent être traduits suivant le principe décrit précédemment : remplacement de l'adresse IP source privée par l'adresse source virtuelle normalisée (IPV) et du port par un nouveau port de substitution attribué à cet usage.

La commande : "PORT IP_ret, P_ret"

où : - IP_ret est l'adresse IP de la connexion en retour ; et

- P_ret le Port de la connexion en retour,

va être traduit en :

20 "PORT IPV, Pv".

où : - IPV est l'adresse source virtuelle, et

- Pv est le port source virtuelle attribué de manière à garantir l'unicité de la connexion.

25 Cette commande va créer une entrée dans la table de conversion effectuant la substitution {IP_ret, P_ret} <=> {IPV, Pv}.

La durée de vie de cette entrée est liée à celle de la connexion de commande FTP.

Si aucune commande PORT n'est envoyée sur le canal de commande, alors IP_ret prend par défaut l'adresse source de la connexion de commande et P_ret prend par défaut la valeur 20 (valeur par défaut des connexions de données associées au protocole FTP).

30 Par ailleurs, pour des raisons de sécurité, RCP et RSH imposent que le port

source prene une valeur inférieure à 1024. En effet, ces ports sont définis comme accessibles uniquement aux utilisateurs ou applications "privilégiés" sur certains systèmes d'exploitation. Le procédé de translation de l'invention doit dans ce cas détecter ces protocoles (par le port destination de la connexion) et attribuer alors un port de substitution d'une valeur inférieure à 1024.

L'invention concerne également un dispositif d'interconnexion mettant en oeuvre le procédé décrit précédemment. Ce dispositif est par exemple inséré dans un routeur IP, permettant l'interconnexion des deux réseaux. Dans ce cas, l'adresse IP normalisée unique pour tout le premier réseau privé 1 est l'adresse de raccordement du routeur IP au second réseau normalisé 2.

En référence à la figure 10, dans un mode de réalisation particulier, le dispositif d'interconnexion de réseaux 11 comprend :

- des moyens (12) de réception et de stockage d'un paquet ;
- des moyens (13) de lecture d'un paquet reçu et stocké, permettant d'identifier une connexion d'origine empruntée par ledit paquet, par la connaissance d'un jeu de paramètres d'identification qui sont les contenus des champs "adresse IP source", "adresse IP destination", "port source", "port destination", et "protocole de transport" du paquet reçu et stocké ;
- au moins une table de conversion (14), associant une connexion transposée distincte à chaque connexion d'origine, chacune desdites connexion d'origine ou transposée étant identifiée par un jeu distinct de paramètres d'identification ;
- des moyens (13) de lecture de ladite table de transposition, permettant de lire le jeu de paramètres d'identification de la connexion transposée associée à la connexion d'origine empruntée par le paquet reçu et stocké ;
- des moyens (15) de modification dudit paquet reçu et stocké permettant de substituer le jeu de paramètres d'identification de la connexion transposée au jeu de paramètres d'identification contenus dans le paquet reçu et stocké, de façon à remplacer la connexion d'origine par la connexion transposée qui lui est associée dans la table de conversion (14).

REVENDICATIONS

1. Procédé d'interconnexion de réseaux mettant chacun en oeuvre la technologie internet, du type permettant d'interconnecter un premier réseau (1) présentant un adressage IP privé et un second réseau (2) présentant un adressage IP normalisé, lesdits
5 premier et second réseaux véhiculant des paquets, chacun desdits paquets comportant un en-tête IP (31) comprenant notamment un champ "adresse IP source" (33) et un champ "adresse IP destination" (34), les paquets étant dits sortants s'ils se déplacent du premier vers le second réseau à travers ledit dispositif et sortants dans le cas contraire, $J_{0,1} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{1,1} = \{IPb, Pb, IPa, Pa, proto\}$,

10 caractérisé en ce que ledit procédé comprend, pour chaque paquet sortant, une première étape de conversion de l'adresse IP privée contenue dans ledit champ "adresse IP source" (33), de façon que ledit champ "adresse IP source" dudit paquet sortant contienne, après conversion, une adresse IP normalisée intermédiaire et unique (IPv) ;

15 et en ce que ledit procédé comprend, pour chaque paquet entrant, une seconde étape de conversion de l'adresse IP normalisée intermédiaire et unique (IPv) contenue dans le champ "adresse IP destination" (34), de façon que ledit champ "adresse IP destination" dudit paquet entrant contienne, après conversion, une des adresses privées du premier réseau.

2. Procédé selon la revendication 1, chacun desdits paquets comportant un en-tête TCP (41) ou UDP (51) comprenant notamment un champ "port source" (42 ; 52) et un
20 champ "port destination" (43 ; 53), ledit en-tête IP (31) comprenant en outre un champ "protocole de transport" (32) indiquant le protocole TCP ou UDP utilisé, les paquets empruntant des connexions bidirectionnelles, chaque connexion étant un lien logique entre une première extrémité (A) du premier réseau (1) et une seconde extrémité (B) du
25 second réseau (2), chaque première ou seconde extrémité étant identifiée par une adresse IP (IPa, IPb), un port (Pa, Pb) et un protocole de transport (proto), chaque connexion (C_{AB}) étant identifiée par un jeu de paramètres $\{IPa, Pa, IPb, Pb, proto\}$ correspondant respectivement à l'adresse IP et au port de la première extrémité (A), à l'adresse IP et au port de la seconde extrémité (B), et au protocole de transport commun aux première et
30 seconde extrémités,

caractérisé en ce que lesdites premières et secondes étapes de conversion d'adresse comprennent, pour chaque paquet, les étapes suivantes :

- lecture (73) des champs "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet, de façon à disposer d'un jeu de paramètres correspondant aux contenus desdits champs lus et permettant d'identifier une connexion d'origine empruntée par ledit paquet ;

- recherche (74) dans une table de conversion (14) d'une entrée correspondant à ladite connexion d'origine empruntée par le paquet, ladite table de conversion associant une connexion transposée distincte à chaque connexion d'origine ;

- s'il n'existe pas d'entrée correspondant à ladite connexion d'origine empruntée par le paquet, création et ajout (76) dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) ;

- modification (77) dudit paquet, de façon à remplacer la connexion d'origine par la connexion transposée qui lui est associée.

3. Procédé selon la revendication 2, caractérisé en ce que ladite étape (76) de création et d'ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) consiste à créer dans ladite table de conversion une première et une seconde entrée associant chacune un jeu de paramètres d'origine $J_o = \{ip_src, p_src, ip_dst, p_dst, p_proto\}$ à un jeu de paramètres transposés $J_t = \{ip_src', p_src', ip_dst', p_dst', p_proto'\}$,

et en ce que, lorsque ladite connexion d'origine est sortante, c'est-à-dire initiée par ladite première extrémité (A) du premier réseau (1), lesdits jeux de paramètres d'origine et transposés s'écrivent respectivement :

- pour ladite première entrée : $J_{o,1} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,1} = \{IPv, Pv, IPb, Pb, proto\}$,

- pour ladite seconde entrée : $J_{o,2} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,2} = \{IPb, Pb, IPa, Pa, proto\}$,

les paramètres IPa, Pa, IPb, Pb et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

les paramètres IPv, Pv et proto définissant une extrémité virtuelle (V), IPv étant ladite adresse IP normalisée intermédiaire et unique et Pv étant un port dont la valeur est calculée en dynamique (83), de façon qu'il n'existe aucune autre connexion de la table de conversion possédant le même couple (IPv, Pv).

4. Procédé selon la revendication 3, caractérisé en ce que, lorsque ladite connexion d'origine est entrante, c'est-à-dire initiée par ladite seconde extrémité (B) du second réseau (2), lesdits jeux de paramètres d'origine et transposés s'écrivent respectivement :

- pour ladite première entrée : $J_{o,1} = \{IPb, Pb, IPv, Pv, proto\}$ et $J_{t,1} = \{IPb, Pb, IPa, Pa, proto\}$,

10 - pour ladite seconde entrée : $J_{o,2} = \{IPa, Pa, IPb, Pb, proto\}$ et $J_{t,2} = \{IPv, Pv, IPb, Pb, proto\}$,

les paramètres IPb, Pb, IPv, Pv et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

15 les paramètres IPv, Pv et proto définissant une extrémité virtuelle (V), IPv appartenant au groupe comprenant ladite adresse IP normalisée intermédiaire et unique, et une adresse IP choisie dans la plage d'adresses normalisées attribuée au site à connecter, et Pv étant un port prédéterminé,

20 et le couple de paramètres (IPa, Pa) étant trouvé (82), grâce au couple de paramètres (IPv, Pv), par lecture d'une table de correspondance statique associant de façon bijective à chaque couple de paramètres (IPa, Pa) parmi une pluralité prédéterminée un couple de paramètres (IPv, Pv) distinct.

5. Procédé selon la revendication 2, caractérisé en ce que ladite étape (76) de création et d'ajout dans ladite table de conversion d'un nouveau couple (connexion d'origine, connexion transposée) consiste à créer dans ladite table de conversion une unique entrée associée à un jeu combiné de paramètres d'origine et transposés $J_c = \{ip_0, p_0, ip_1, p_1, ip_2, p_2, proto\}$,

25 et en ce que, lorsque ladite connexion d'origine est sortante, c'est-à-dire initiée par ladite première extrémité (A) du premier réseau (1), ledit jeu combiné de paramètres d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, proto\}$,

30

les paramètres IPa, Pa, IPb, Pb et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

5 les paramètres IPv, Pv et proto définissant une extrémité virtuelle (V), IPv étant ladite adresse IP normalisée intermédiaire et unique, et Pv étant un port dont la valeur est calculée en dynamique (83), de façon qu'il n'existe aucune autre connexion de la table de conversion possédant le même couple (IPv, Pv).

6 . Procédé selon la revendication 5, caractérisé en ce que, lorsque ladite connexion d'origine est entrante, c'est-à-dire initiée par ladite seconde extrémité (B) du second
10 réseau (2), ledit jeu combiné de paramètres d'origine et transposés s'écrit $J_c = \{IPa, Pa, IPb, Pb, IPv, Pv, proto\}$,

les paramètres IPb, Pb, IPv, Pv et proto étant lus dans les champs respectivement "adresse IP source", "port source", "adresse IP destination", "port destination", et "protocole de transport" dudit paquet,

15 les paramètres IPv, Pv et proto définissant une extrémité virtuelle (V), IPv appartenant au groupe comprenant ladite adresse IP normalisée intermédiaire et unique, et une adresse IP choisie dans la plage d'adresses normalisées attribuée au site à connecter, et Pv étant un port prédéterminé,

et le couple de paramètres (IPa, Pa) étant trouvé (82), grâce au couple de paramètres (IPv, Pv), par lecture d'une table de correspondance statique associant de façon bijective
20 à chaque couple de paramètres (IPa, Pa) parmi une pluralité prédéterminée un couple de paramètres (IPv, Pv) distinct.

7 . Procédé selon l'une quelconque des revendications 3 et 4, caractérisé en ce que, pour chaque paquet sortant, ladite étape (77) de modification du paquet consiste à
25 remplacer (93) le contenu des champs "adresse IP source" et "port source" du paquet par les paramètres correspondants ip_src' et p_src' dudit jeu de paramètres transposés J_t d'identification de la connexion transposée,

et en ce que, pour chaque paquet entrant, ladite étape (77) de modification du paquet consiste à remplacer (94) le contenu des champs "adresse IP destination" et "port
30 destination" du paquet par les paramètres correspondants ip_dst' et p_dst' dudit jeu de

paramètres transposés J_t d'identification de la connexion transposée.

8. Procédé selon l'une quelconque des revendications 5 et 6, caractérisé en ce que, pour chaque paquet sortant, ladite étape de modification du paquet consiste à remplacer le contenu des champs "adresse IP source" et "port source" du paquet par les paramètres ip_2 et p_2 dudit jeu combiné de paramètres d'origine et transposés J_c .

et en ce que, pour chaque paquet entrant, ladite étape de modification du paquet consiste à remplacer le contenu des champs "adresse IP destination" et "port destination" du paquet par les paramètres ip_0 et p_0 dudit jeu combiné de paramètres d'origine et transposés J_c .

9. Procédé selon l'une quelconque des revendications 2 à 8, caractérisé en ce que ladite table de conversion (14) est mise à jour de façon dynamique selon une stratégie prédéterminée de mise à jour.

10. Procédé selon la revendication 9, caractérisé en ce que ladite stratégie prédéterminée de mise à jour consiste à ne laisser chaque couple (110, 111) de connexions d'origine et transposée inscrit dans la table de conversion qu'entre un instant de début et un instant de fin de vie de ladite connexion d'origine.

11. Procédé selon la revendication 10, caractérisé en ce que, dans le cas d'une connexion utilisant le protocole TCP, lesdits instants de début et de fin de vie de la connexion d'origine sont déterminés en se référant au diagramme d'état d'une session TCP, selon la spécification TCP (RFC 793).

12. Procédé selon l'une quelconque des revendications 10 et 11, caractérisé en ce que, dans le cas d'une connexion utilisant le protocole UDP, ledit instant de début de vie de la connexion d'origine est déterminé par le passage, dans un sens donné, d'un paquet de requête, et en ce que ledit instant de fin de vie est déterminé par le passage, dans le sens inverse dudit sens donné, d'un paquet de réponse.

13. Procédé selon l'une quelconque des revendications 10 et 11, caractérisé en ce que, dans le cas d'une connexion utilisant le protocole UDP, ledit instant de début de vie de la connexion d'origine est déterminé par le passage, dans un sens donné, d'un paquet de requête, et en ce que ledit instant de fin de vie est déterminé par l'écoulement d'une durée prédéterminée depuis ledit instant de début de vie.

14. Procédé selon la revendication 9, caractérisé en ce que ladite stratégie prédéterminée de mise à jour consiste à :

- créer une connexion lorsqu'apparaît un nouveau paquet n'appartenant à aucune connexion existante ;
- 5 - maintenir constamment une variable définissant l'heure du dernier paquet ayant transité sur cette connexion ;
- lorsque la table contient un nombre prédéterminé de connexions simultanées, supprimer de la table l'entrée correspondant à la connexion dont la variable notant l'heure du dernier paquet est la plus ancienne.

10 15. Procédé selon l'une quelconque des revendications 2 à 14, caractérisé en ce qu'il comprend une étape de filtrage des paquets sortants en fonction du contenu d'un des champs appartenant au groupe comprenant les champs "adresse IP source", "adresse IP destination" et "port destination".

15 16. Dispositif d'interconnexion de réseaux mettant chacun en oeuvre la technologie internet, du type destiné à être inséré entre un premier réseau (1) présentant un adressage IP privé et un second réseau (2) présentant un adressage IP normalisé, lesdits premier et second réseaux véhiculant des paquets, chacun desdits paquets comportant un en-tête IP (31) comprenant notamment un champ "adresse IP source" (33) et un champ "adresse IP destination" (34), les paquets étant dits sortants s'ils se déplacent du premier vers le

20 second réseau à travers ledit dispositif et sortants dans le cas contraire,

caractérisé en ce que ledit dispositif (11) possède une adresse IP normalisée intermédiaire et unique (IPv) dans ledit second réseau,

et en ce qu'il comprend notamment :

- des premiers moyens de conversion des adresses IP privées contenues dans les
- 25 champs "adresse IP source" des paquets sortants, de façon que ledit champ "adresse IP source" de chacun desdits paquets sortants contienne, après conversion, ladite adresse IP normalisée intermédiaire et unique (IPv) ; et
- des seconds moyens de conversion de l'adresse IP normalisée intermédiaire et unique (IPv) contenue dans les champs "adresse IP destination" des paquets entrants, de
- 30 façon que ledit champ "adresse IP destination" de chacun desdits paquets entrants

contienne, après conversion, une des adresses privées du premier réseau.

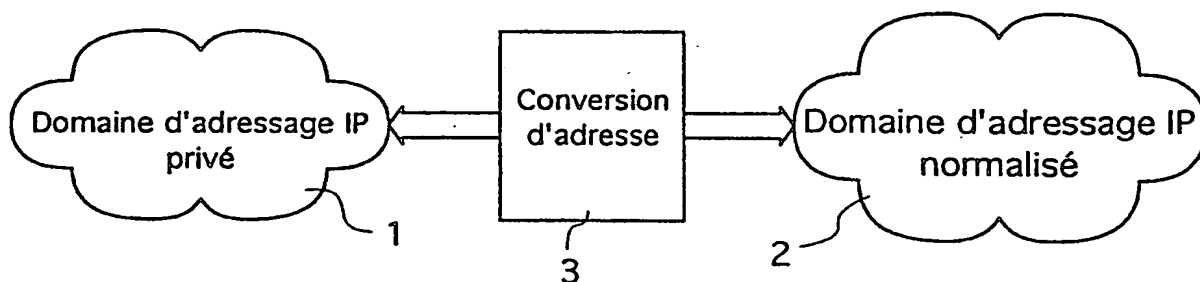
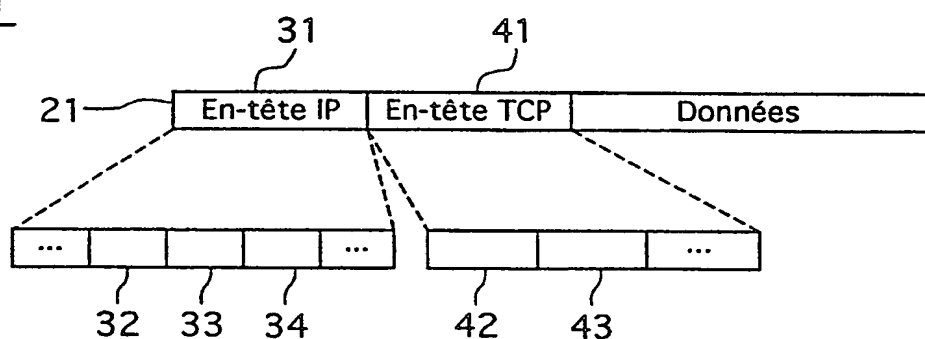
17. Dispositif selon la revendication 16, chacun desdits paquets comportant un en-tête TCP (41) ou UDP (51) comprenant notamment un champ "port source" (42 ; 52) et un champ "port destination" (43 ; 53), ledit en-tête IP (31) comprenant en outre un champ "protocole de transport" (32) indiquant le protocole TCP ou UDP utilisé,

caractérisé en ce que lesdits premiers et seconds moyens de conversion d'adresse comprennent :

- des moyens (12) de réception et de stockage d'un paquet ;
- des moyens (13) de lecture d'un paquet reçu et stocké, permettant d'identifier une connexion d'origine empruntée par ledit paquet, par la connaissance d'un jeu de paramètres d'identification qui sont les contenus des champs "adresse IP source", "adresse IP destination", "port source", "port destination", et "protocole de transport" du paquet reçu et stocké ;
- au moins une table de conversion (14), associant une connexion transposée distincte à chaque connexion d'origine, chacune desdites connexion d'origine ou transposée étant identifiée par un jeu distinct de paramètres d'identification ;
- des moyens (13) de lecture de ladite table de transposition, permettant de lire le jeu de paramètres d'identification de la connexion transposée associée à la connexion d'origine empruntée par le paquet reçu et stocké ;
- des moyens (15) de modification dudit paquet reçu et stocké permettant de substituer le jeu de paramètres d'identification de la connexion transposée au jeu de paramètres d'identification contenus dans le paquet reçu et stocké, de façon à remplacer la connexion d'origine par la connexion transposée qui lui est associée dans la table de conversion.

18. Routeur IP d'interconnexion de réseaux, caractérisé en ce qu'il comprend un dispositif (11) selon l'une quelconque des revendications 16 et 17, ladite adresse IP normalisée intermédiaire et unique (IPv) étant l'adresse IP normalisée de raccordement dudit routeur IP audit second réseau (2).

1/5

Fig. 1Fig. 2

	Longueur (en bits)	Signification
42	16	Port source
43	16	Port destination
	32	N° de séquence
	32	N° d'acquittement
	4	Longueur en-tête
	6	Réservé
	6	Drapeaux
	16	Fenêtre
44	16	Total de contrôle
	16	Pointeur d'urgence
	Variables	Options
	Variables	Données

Fig. 4

	Longueur (en bits)	Signification
	4	Version
	4	Longueur de l'en-tête
	8	Type de service
	16	Longueur total
	16	Identification
	2	Drapeaux
	14	Déplacement Fragment
	8	Durée de vie
32	8	Protocole
34	16	Total de contrôle en-tête
33	32	Adresse IP source
34	32	Adresse IP destination
	Variable	Options
	Variable	Données

Fig. 3

2/5

51

	Longueur (en bits)	Signification
52	16	Port source
53	16	Port destination
	16	Longueur du message
54	16	Total de contrôle
	Variable	Données

Fig. 5

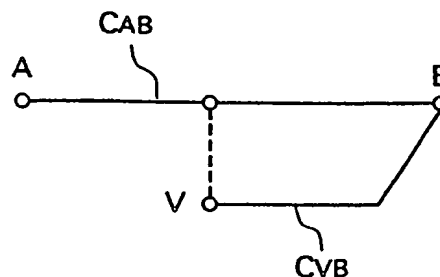


Fig. 6

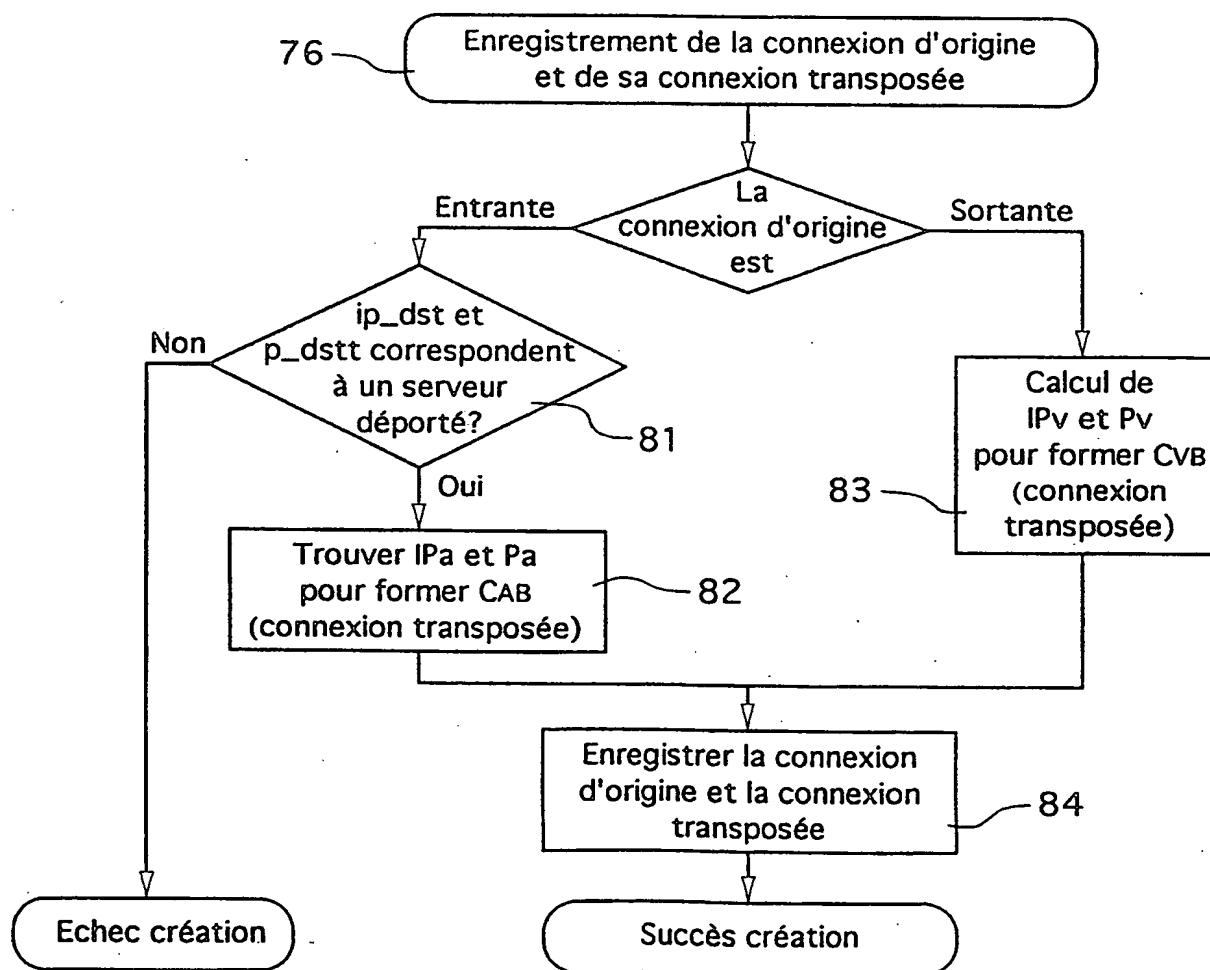


Fig. 8

3/5

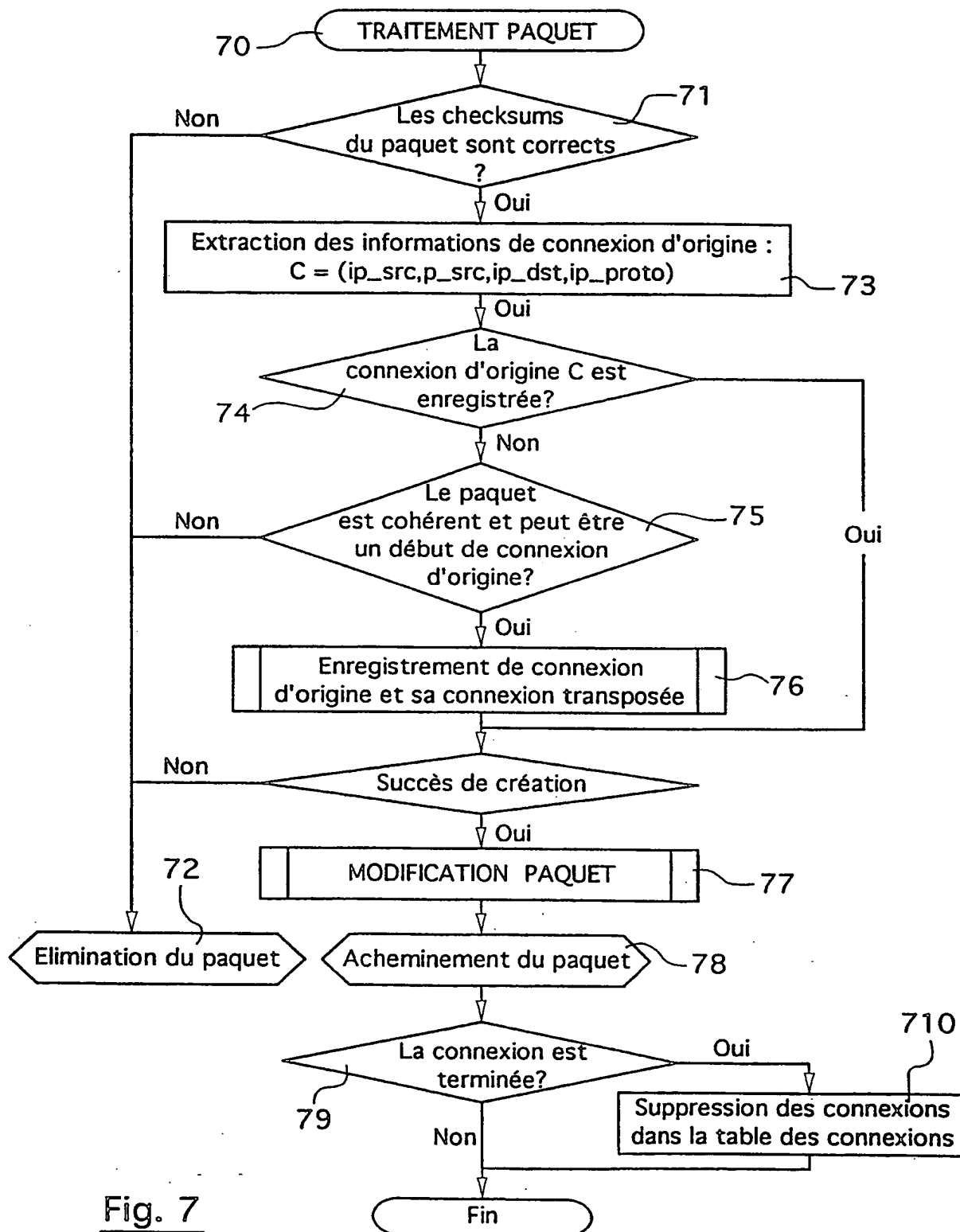


Fig. 7

4/5

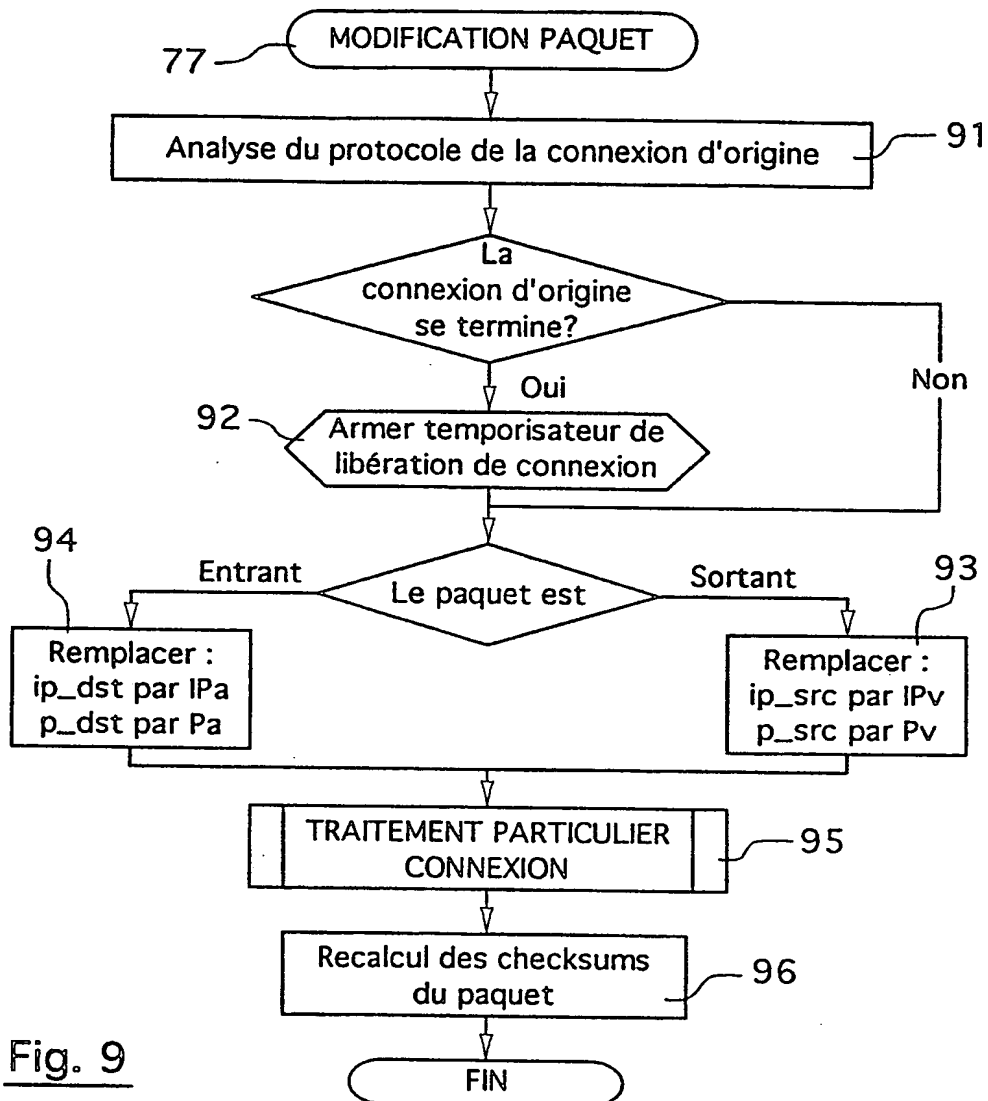


Fig. 9

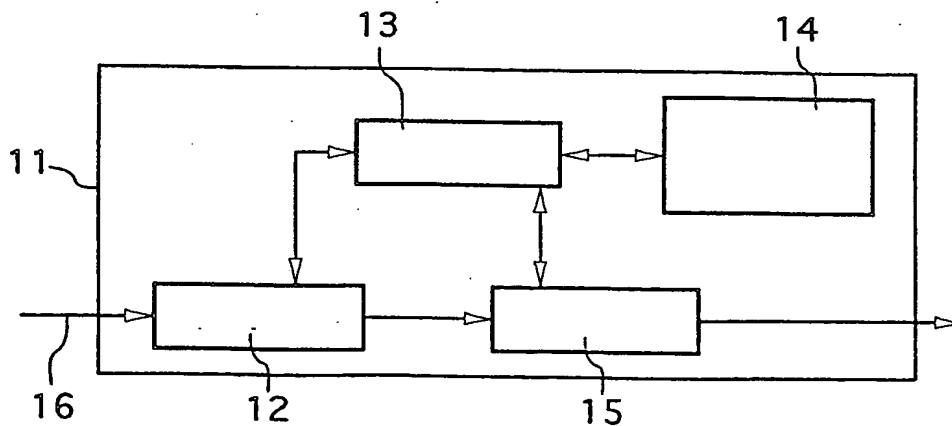
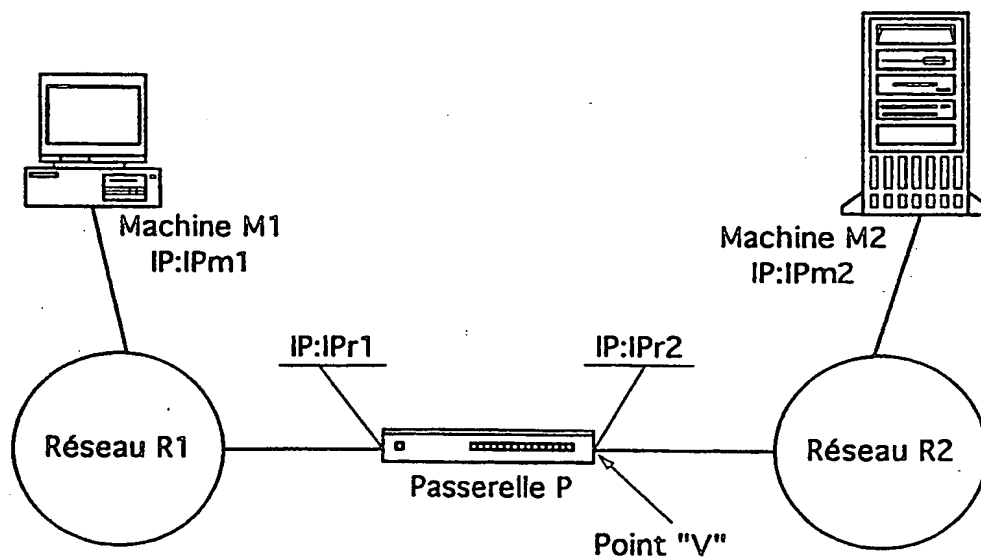


Fig. 10

5/5

14

CONNEXIONS D'ORIGINE					CONNEXIONS TRANSPOSEES						
ip_src	p_src	ip_dst	p_dst	proto	ip_src'	p_src'	ip_dst'	p_dst'	proto'		
J0,1	IPa	Pa	IPb	Pb	proto	IPv	Pv	IPb	Pb	proto	Jt,1
J0,2	IPb	Pb	IPv	Pv	proto	IPb	Pb	IPa	Pa	proto	Jt,2

Fig. 11Fig. 12

INTERNATIONAL SEARCH REPORT

International Application No

PLI/FR 96/01179

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04L29/06 H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, vol. 8, no. 1, January 1990, NEW YORK, US, pages 67-79, XP000133533 L.SVOBODOVA ET AL: "HETEROGENEITY AND OSI" see paragraph IV.B see paragraph V	1,16
A	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, vol. 8, no. 1, January 1990, NEW YORK, US, pages 4-11, XP000133530 C.A.SUNSHINE: "NETWORK INTERCONNECTION AND GATEWAYS" see paragraph I.C see paragraph III	1,16

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

A document member of the same patent family

Date of the actual completion of the international search

25 September 1996

Date of mailing of the international search report

04. 10. 96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax (+31-70) 340-3016

Authorized officer

Canosa Arete, C

RAPPORT DE RECHERCHE INTERNATIONALE

De: 'e Internationale No
PCT/FR 96/01179

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L29/06 H04L12/66

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, vol. 8, no. 1, Janvier 1990, NEW YORK, US, pages 67-79, XP000133533 L.SVOBODOVA ET AL: "HETEROGENEITY AND OSI" voir alinéa IV.B voir alinéa V ---	1,16
A	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, vol. 8, no. 1, Janvier 1990, NEW YORK, US, pages 4-11, XP000133530 C.A.SUNSHINE: "NETWORK INTERCONNECTION AND GATEWAYS" voir alinéa I.C voir alinéa III -----	1,16

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

25 Septembre 1996

Date d'expédition du présent rapport de recherche internationale

04.10.96

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+ 31-70) 340-3016

Fonctionnaire autorisé

Canosa Arete, C